

Claims

1. A computer-implemented method for blockchain address mapping, to be performed by a system for blockchain address mapping, comprising:

obtaining, from a client, one or more local accounts, one or more identifications of one or more blockchains, and one or more requests for creating in the one or more blockchains a plurality of blockchain addresses in association with the one or more local accounts, wherein the client corresponds to the one or more local accounts in the system;

generating a plurality of public-private key pairs respectively for the plurality of blockchain addresses to be created;

creating the plurality of blockchain addresses respectively in the one or more blockchains, in association with the one or more local accounts and a plurality of public keys of the plurality of public-private key pairs; and

transmitting a notification to the client for the client to correspondingly store the one or more local accounts in association with the one or more identifications of the one or more blockchains, wherein:

the notification comprises the one or more local accounts for which the plurality of blockchain addresses are created and the one or more corresponding identifications of the one or more blockchains, and

the plurality of blockchain addresses and a plurality of private keys of the plurality of public-private key pairs are stored in the system and are not stored at the client.

2. The method of claim 1, wherein:

obtaining the one or more local accounts, the one or more identifications of the one or more blockchains, and the one or more requests comprises: obtaining the one or more requests for creating the plurality of blockchain addresses in a plurality of blockchains in association with one local account; and

creating the plurality of blockchain addresses respectively in the one or more blockchains in association with the one or more local accounts comprises: correspondingly in the plurality of

blockchains, creating in a batch the plurality of blockchain addresses in association with the one local account.

3. The method of claim 1, wherein:

obtaining the one or more local accounts, the one or more identifications of the one or more blockchains, and the one or more requests comprises: obtaining the one or more requests for creating the plurality of blockchain addresses in one blockchain in association with a plurality of local accounts; and

creating the plurality of blockchain addresses respectively in the one or more blockchains in association with the one or more local accounts comprises: in the one blockchain, creating in a batch the plurality of blockchain addresses in association with the plurality of the local accounts.

4. The method of claim 1, wherein:

obtaining the one or more local accounts, the one or more identifications of the one or more blockchains, and the one or more requests comprises: obtaining the one or more requests for creating the plurality of blockchain addresses in a plurality of blockchains in association with a plurality of local accounts; and

creating the plurality of blockchain addresses respectively in the one or more blockchains in association with the one or more local accounts comprises: correspondingly in the plurality of blockchains, creating in a batch the plurality of blockchain addresses in association with the plurality of the local accounts.

5. The method of claim 1, further comprising:

storing a plurality of mapping relationships among the one or more local accounts, the plurality of created blockchain addresses, the plurality of public-private key pairs, and the one or more identifications of the one or more blockchains.

6. The method of claim 1, wherein creating the plurality of blockchain addresses respectively in the one or more blockchains, in association with the one or more local accounts and the plurality of public keys of the plurality of public-private key pairs comprises:

constructing a blockchain transaction comprising the plurality of public keys; and
sending the blockchain transaction to one or more blockchain nodes of the one or more
blockchains according to the one or more identifications to create the plurality of blockchain
addresses respectively based on the plurality of public keys.

7. The method of claim 1, wherein generating the plurality of public-private key pairs
respectively for the plurality of blockchain addresses to be created comprises:

for each of the plurality of blockchain addresses, generating a public-private key pair and
encrypting a private key of the public-private key pair.

8. The method of claim 7, wherein generating the public-private key pair and encrypting
the private key of the public-private key pair comprises:

in a Trusted Execution Environment (TEE), generating the public-private key pair and
encrypting the private key of the public-private key pair.

9. The method of claim 7, wherein creating the plurality of blockchain addresses
respectively in the one or more blockchains, in association with the one or more local accounts
and the plurality of public keys of the plurality of public-private key pairs further comprises:

for each of the plurality of blockchain addresses, storing the encrypted private key in a
Key Management System (KMS).

10. The method of claim 7, further comprising:

for each of the plurality of blockchain addresses, storing a mapping relationship among
one of the local accounts, the each of the blockchain addresses, a corresponding Key
Management System (KMS) directory, and one of the identifications, wherein the KMS directory
links to the corresponding encrypted private key.

11. The method of claim 1, wherein obtaining the one or more local accounts, the one or
more identifications of the one or more blockchains, and the one or more requests comprises:

obtaining, from the client, the one or more local accounts in accordance with a Lightweight Directory Access Protocol (LDAP).

12. A system for blockchain address mapping, comprising one or more processors and one or more non-transitory computer-readable memories coupled to the one or more processors and configured with instructions executable by the one or more processors to cause the system to perform operations comprising:

obtaining, from a client, one or more local accounts, one or more identifications of one or more blockchains, and one or more requests for creating in the one or more blockchains a plurality of blockchain addresses in association with the one or more local accounts, wherein the client corresponds to the one or more local accounts in the system;

generating a plurality of public-private key pairs respectively for the plurality of blockchain addresses to be created;

creating the plurality of blockchain addresses respectively in the one or more blockchains, in association with the one or more local accounts and a plurality of public keys of the plurality of public-private key pairs; and

transmitting a notification to the client for the client to correspondingly store the one or more local accounts in association with the one or more identifications of the one or more blockchains, wherein:

the notification comprises the one or more local accounts for which the plurality of blockchain addresses are created and the one or more corresponding identifications of the one or more blockchains, and

the plurality of blockchain addresses and a plurality of private keys of the plurality of public-private key pairs are stored in the system and are not stored at the client.

13. The system of claim 12, wherein:

obtaining the one or more local accounts, the one or more identifications of the one or more blockchains, and the one or more requests comprises: obtaining the one or more requests for creating the plurality of blockchain addresses in a plurality of blockchains in association with a plurality of local accounts; and

creating the plurality of blockchain addresses respectively in the one or more blockchains in association with the one or more local accounts comprises: correspondingly in the plurality of blockchains, creating in a batch the plurality of blockchain addresses in association with the plurality of the local accounts.

14. The system of claim 12, wherein the operations further comprise:

storing a plurality of mapping relationships among the one or more local accounts, the plurality of created blockchain addresses, the plurality of public-private key pairs, and the one or more identifications of the one or more blockchains.

15. A non-transitory computer-readable storage medium for blockchain address mapping, the storage medium associated with a system for blockchain address mapping, the storage medium configured with instructions executable by one or more processors to cause the one or more processors to perform operations comprising:

obtaining, from a client, one or more local accounts, one or more identifications of one or more blockchains, and one or more requests for creating in the one or more blockchains a plurality of blockchain addresses in association with the one or more local accounts, wherein the client corresponds to the one or more local accounts in the system;

generating a plurality of public-private key pairs respectively for the plurality of blockchain addresses to be created;

creating the plurality of blockchain addresses respectively in the one or more blockchains, in association with the one or more local accounts and a plurality of public keys of the plurality of public-private key pairs; and

transmitting a notification to the client for the client to correspondingly store the one or more local accounts in association with the one or more identifications of the one or more blockchains, wherein:

the notification comprises the one or more local accounts for which the plurality of blockchain addresses are created and the one or more corresponding identifications of the one or more blockchains, and

the plurality of blockchain addresses and a plurality of private keys of the plurality of public-private key pairs are stored in the system and are not stored at the client.

16. The storage medium of claim 15, wherein:

obtaining the one or more local accounts, the one or more identifications of the one or more blockchains, and the one or more requests comprises: obtaining the one or more requests for creating the plurality of blockchain addresses in a plurality of blockchains in association with one local account; and

creating the plurality of blockchain addresses respectively in the one or more blockchains in association with the one or more local accounts comprises: correspondingly in the plurality of blockchains, creating in a batch the plurality of blockchain addresses in association with the one local account.

17. The storage medium of claim 15, wherein the operations further comprise:

storing a plurality of mapping relationships among the one or more local accounts, the plurality of created blockchain addresses, the plurality of public-private key pairs, and the one or more identifications of the one or more blockchains.

18. The storage medium of claim 15, wherein:

obtaining the one or more local accounts, the one or more identifications of the one or more blockchains, and the one or more requests comprises: obtaining the one or more requests for creating the plurality of blockchain addresses in one blockchain in association with a plurality of local accounts; and

creating the plurality of blockchain addresses respectively in the one or more blockchains in association with the one or more local accounts comprises: in the one blockchain, creating in a batch the plurality of blockchain addresses in association with the plurality of the local accounts.